

REMARKS

The above referenced patent application has been reviewed in light of the Office Action, dated May 03, 2004, in which:

- the title of the specification is objected to as not being properly descriptive;
- claims 38 and 40 are objected to due to minor informalities;
- claims 28, 31, 36, 39, 42, and 46 are rejected under 35 U.S.C. § 112, 2nd paragraph;
- claims 28, 32, and 33 are rejected under 35 U.S.C. § 102(b) on Feistel (US Patent No. 4,316,055); and
- claims 29-31, 34-37, 39, and 41-47 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Feistel, alone.

Reconsideration of the above referenced patent application in view of the foregoing amendments and the following remarks is respectfully requested.

A Petition for Extension of Time in order to extend the period for response 3 month(s), including the appropriate fee, is filed herewith.

Claims 28-47 are now pending the above referenced patent application. No claims have been cancelled, or added. Claims 28, 31, 36, 38-40, 42, and 46 have been amended; however, these amendments are merely directed to matters of form, and, therefore, do not result in prosecution history estoppel and do not alter the scope of the claims.

1. Miscellaneous Objections

1.1. Title Objection

The title was objected to as non-descriptive. Please replace the original title "A Dual Use Block/Stream Cipher" with the Examiner's suggested title, "Dual Use Block/Stream Cipher Apparatus Using A Key Section To Provide A Key Stream To A Data Section." Applicants submit that both the original title and the suggested title of the March 1, 2004 Amendment are indicative of the invention as recited in the claims; however, rather than belabour the point, Applicants have amended the title to address the PTO's concerns. It is respectfully asserted that these amendments are merely directed to matters of form, and, therefore, do not result in prosecution history estoppel and do not alter the scope of the claims. Therefore, Applicants respectfully request that the objection be withdrawn.

1.2. Claim Objections: Claims 38 and 40

Although Applicants respectfully disagree that these claims are informal, rather than belabour the point, Applicants have amended the claims to address the PTO's concerns. It is respectfully asserted that these amendments are merely directed to matters of form, and, therefore, do not result in prosecution history estoppel and do not alter the scope of the claims. It is respectfully requested that the foregoing claim objection be withdrawn.

2. 35 U.S.C. § 112, 2nd paragraph

2.1. Claims 28, 31, 36, 39, 42, and 46

The PTO has rejected claims 28, 31, 36, 39, 42, and 46 under 35 U.S.C. § 112, 2nd paragraph. Although Applicants respectfully disagree that these claims are indefinite, rather than belabour the point, Applicants have amended the claims to address the PTO's concerns. It is respectfully asserted that these amendments are merely directed to matters of form, and, therefore, do not result in prosecution history estoppel and do not alter the scope of the claims. It is respectfully requested that the foregoing claim rejections be withdrawn.

3. 35 U.S.C. § 102

3.1. *Feistel: Claims 28, 32, and 33*

The PTO has rejected claims 28, 32, and 33 under 35 U.S.C. § 102(b) as being anticipated by Feistel. This rejection by the PTO of these claims is respectfully traversed.

It is well-established that in order to establish a *prima facie* case of anticipation under § 102 of the patent statute, the PTO must provide a single prior art document that alone has every element and every limitation of the claim being rejected. Therefore, if even a single element or limitation is not met by the asserted document, then the PTO has not succeeded in establishing a *prima facie* case.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Brothers v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Applicants begin with claim 28. Claim 28, as amended, recites:

1 28: (Currently Amended) An encoding apparatus comprising:
2 a block cipher key section to be initialized with a block cipher key, having
3 transformation units to transform the block cipher key (a transformed block cipher key);
4 a data section coupled with the block cipher key section to be initialized with a
5 random number, having transformation units to transform the random number based on
6 the transformed block cipher key;
7 a stream cipher key section coupled with the block cipher key section to modify
8 the block cipher key according to a stream cipher key to produce data bits to dynamically
9 modify the random number (a modified random number) in the data block section; and
10 a mapping section to receive the modified random number and the transformed
11 block cipher key and generate a pseudo random bit sequence based on the modified
12 random number and the transformed block cipher key.

It is respectfully asserted that, as just one example of how the text cited by the PTO fails to meet the language of the rejected claims, Feistel does not show, teach, use, or describe a stream cipher key section coupled with the block cipher key section to modify the block cipher key. Feistel instead shows a stream and a block sections which operate relatively independent of each other. See Feistel Fig. 3, elements 3-7 for the stream section, and Fig. 4 for the block section. Feistel does not use the stream section to modify the block cipher key as illustrated by Applicants Fig. 1. Applicants respectfully contend that Feistel fails to satisfy a *prima facie* case of anticipation as directed by 35 U.S.C. § 102.

Claims 32 and 33 either depend from claim 28, or include a substantially similar and patentably distinct limitation as claim 28. It is, therefore, respectfully requested that the rejection of these claims also be withdrawn.

4. 35 U.S.C. § 103(a)

4.1. *Feistel: Claims 29-31, 34-37, 39, and 41-47*

The PTO has also rejected claims 29-31, 34-37, 39, and 41-47 under 35 U.S.C. § 103(a) based upon Feistel, alone. The rejection of these claims is respectfully traversed.

M.P.E.P. § 706.02(j) sets forth the standard for a § 103(a) rejection:

To establish a prima facie case of obviousness, three basic criteria must be met.

First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine reference teachings.

Second, there must be a reasonable expectation of success.

Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) (whitespace added).

Applicants begin with claim 29. Claim 29 recites:

1 29: (Previously Presented) An apparatus according to claim 28, wherein the block cipher key
2 section further includes first, second, and third registers, to be collectively initialized with the
3 block cipher key.

Claim 29 ultimately depends from the independent claim 28. Claim 28, as amended,
recites:

1 28: (Currently Amended) An encoding apparatus comprising:
2 a block cipher key section to be initialized with a block cipher key, having transformation
3 units to transform the block cipher key (a transformed block cipher key);
4 a data section coupled with the block cipher key section to be initialized with a random
5 number, having transformation units to transform the random number based on the transformed
6 block cipher key;
7 a stream cipher key section coupled with the block cipher key section to modify the block
8 cipher key according to a stream cipher key to produce data bits to dynamically modify the

9 random number (a modified random number) in the data block section; and
10 a mapping section to receive the modified random number and the transformed block
11 cipher key and generate a pseudo random bit sequence based on the modified random number and
12 the transformed block cipher key.

Applicants respectfully assert that the combination set forth by the PTO fails to meet the requirement for a *prima facie* case for a § 103(a) rejection for at least the following reasons.


It is respectfully asserted that, as just one example of how the text cited by the PTO fails to meet the language of the rejected claims, Feistel does not show, teach, use, or describe a stream cipher key section coupled with the block cipher key section to modify the block cipher key. Feistel instead shows a stream and a block sections which operate relatively independent of each other. See Feistel Fig. 3, elements 3-7 for the stream section, and Fig. 4 for the block section. Feistel does not use the stream section to modify the block cipher key as illustrated by Applicants Fig. 1. Therefore, Applicants respectfully assert that Feistel fails to produce the invention as recited in the rejected claims. It is, therefore, respectfully requested that the rejection of this claim be withdrawn.

Claims 30, 31, 34-37, 39, and 41-47 either depend from and include the limitations of claim 29, or include a substantially similar and patentably distinct limitation as claim 29. Therefore, these claims patentably distinguish from the cited patents on the same basis as claim 29. It is, therefore, respectfully requested that the PTO withdraw the rejections of these claims.

CONCLUSION

In view of the foregoing, it is respectfully asserted that all claims pending in this application, as amended, are in condition for allowance. If the Examiner has any questions, they are invited to contact the undersigned at 503-264-7002. Reconsideration of this patent application and early allowance of all claims is respectfully requested.

Respectfully submitted,


Justin B. Scout
Reg. No. 54,431

Dated:

Tue 11/02/04

c/o Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Blvd., Seventh Floor
Los Angeles, CA 90025-1026
(503) 264-0967

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Commissioner for Patents, P.O. Box 100, Alexandria, VA 22313 on:

11/3/04

Date of Deposit

Lamara Simpson
Name of Person Mailing Correspondence

Lamara Simpson 11/3/04
Signature Date